




<b>G001</b>	<b>Privacy Policy</b>
<b>Purpose</b>	To outline the Free Reformed School Association's (FRSA) and Schools obligations in dealing with entrusted information.
<b>Authority</b>	Commonwealth Privacy Act 1998 Criminal Code School Education Act 1999 and School Education Regulations 2018 (as updated annually)
<b>Policy</b>	Personal information about individuals held by the FRSA and Schools will be kept up to date and used in accordance with the GP001 Privacy Procedure.
<b>Delegation</b>	The CEO, Principals, and Administration Manager
<b>Related Policies</b>	G007 Record Management CP003 Access to Students CP004 Use of Photographs Proc006 Enrolment IT005 Password
<b>Date approved</b>	October 2008; November 2011, July 2015, June 2018
<b>Next Review Due</b>	May 2021
<b>Review Authority</b>	Governance
<b>Keywords</b>	Privacy; records; personal information;

<b>Authorised by:</b>	
<b>Board Chairman</b>	H Dykstra
<b>Date:</b>	May 2018



This Privacy Procedure applies to schools conducted by the Free Reformed School Association (FRSA) and sets out how the FRSA and each school manages personal information provided to or collected by it.

The FRSA and Schools are bound by the Australian Privacy Principles (AAP's) contained in the Commonwealth *Privacy Act 1988*.

The FRSA may, from time to time, review and update this Privacy Procedure to take account of new laws and technology, changes to schools' operations and practices and to make sure it remains appropriate to the changing school environment.

The FRSA and Schools approach to Privacy has at its core:

1. A commitment from all staff, Council, Committee and Board members to promote and comply with the Australian Privacy Principles
2. An expectation that matters of concern will be resolved through effective management, communication and consultation.

**The FRSA and Senior Staff are responsible for** complying with the Australian Privacy Principles (APP's) and the Commonwealth Privacy Act (1998).

This responsibility is to be discharged by:

- Promoting awareness of the APP's and the Commonwealth Privacy Act (1988)
- Managing personal information in an open and transparent way
- Taking such steps as are reasonable in the circumstances to implement policy, procedures, practices and systems relating to the FRSA and School's functions or activities that will:
  - Ensure compliances with the APP's
  - Enable the FRSA (and Schools) to deal with inquiries or complaints about compliance with the APP's
- Having a clearly expressed and up-to-date Privacy Policy and associated documents about the FRSA's and Schools managements of personal information
- If it is lawful or practicable, give individuals the option of interacting anonymously with the FRSA and School's by using a pseudonym
- Only collecting personal information that is reasonably necessary for achieving the FRSA's and School's objective and directly related activities
- Using fair and lawful means to collect personal information
- Collecting personal information directly from an individual if it is reasonable and practicable to do so
- At the time the FRSA and School's collect personal information or as soon as practical afterwards, take such steps (if any) as are reasonable in the circumstances to make an individual aware of
  - Why the information is being collected
  - Who else the information may be shared with
  - Any other relevant matters
- Only using or disclosing personal information for the primary purpose of the collection unless one of the exceptions in APP 6.2 applies (for example, for a related secondary purpose within the individual's reasonable expectations, the FRSA or School has consent or there are specific

law enforcement or public health or public safety circumstances). If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.

- Not using personal information for direct marketing, unless one of the exceptions in APP 7 applies (for example, the FRSA or School has obtained consent or where the individual has a reasonable expectation of the information being used or disclosed for that purpose and the FRSA or School has provided a simple means for the individual to unsubscribe from such communications).
- Taking such steps (if any) as are reasonable in the circumstances to ensure the personal information the FRSA or School collects, uses or discloses is accurate, complete and up-to-date. This may require the FRSA or School to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.
- Taking such steps as are reasonable in the circumstance to protect the personal information the FRSA or School holds from misuse, interference and loss from unauthorised access, modification or disclosure.
- Taking such steps as are reasonable in the circumstance to destroy or permanently de-identify personal information no longer needed for any purpose for which the FRSA or School may use or disclose the information.
- If requested, the FRSA or School must give access to the personal information it holds about an individual unless particularly circumstances apply that allow it to limit the extent to which it gives access.
- Reviewing all electronic and paper-based systems for compliance with the APP's (for example the membership database, finance systems, electronic communication etc)
- Managing suspected or actual data breaches in accordance with the data breach response plan and requirements of the Australian Privacy Commissioner.

**The Principal is responsible for** complying with the Australian Privacy Principles and the Commonwealth Privacy Act (1998).

This responsibility is to be discharged at the local school level by:

- Promoting awareness of the APP's and the Commonwealth Privacy Act (1988)
- Promoting awareness of the FRSA Privacy Policy, Procedure and associated supporting documents amongst staff, Council members and committee members (as appropriate)
- Ensuring that Government related identifiers are not adopted, used or disclosed unless one of the exceptions applies (for example the use of disclosure is reasonably necessary to verify the identity of the individual for the purposes of the School's functions or activities)
- Reviewing all electronic and paper-based systems for compliance with the APP's (for example SEQTA)
- Managing suspected or actual data breaches in accordance with the data breach response plan and requirements of the Australian Privacy Commissioner.

**Individual staff (teachers, education assistants, management and administration), Council, Committee and Board members are responsible for** complying with the Australian Privacy Principles and the Commonwealth Privacy Act (1998).

This responsibility is to be discharged by:

- Promoting awareness of the APP's and the Commonwealth Privacy Act (1988)
- Managing personal information in an open and transparent way
- Taking such steps as are reasonable in the circumstances to implement approved policies, procedures, practices and systems relating to the FRSA and School's functions or activities that will:
  - Ensure compliance with the APPs

- Enable the FRSA (and Schools) to deal with inquiries or complaints about compliance with the APP's
- Taking such steps as outlined in relevant policies (for example password policy) to ensure that access to systems that hold personal information are not compromised
- Maintaining confidentiality and protecting the privacy of personal and sensitive information
- Referring requests for personal information to the Principal or Manager
- Reporting suspected or actual data breaches in accordance with the Data Breach Response Breach Plan.

This procedure is supported by the following documents:

1. Privacy Fact Sheet
2. Data Breach Response Plan
3. Privacy Compliance Manual



## Appendix 1

## Privacy Fact Sheet

### Introduction

This Fact Sheet outlines the personal information collected by the FRSA and the Schools and how this information is used, protected and if applicable shared.

### **What kinds of personal information does the FRSA and Schools collect and how does the FRSA and Schools collect it?**

The type of information the FRSA and schools collect, and hold includes (but is not limited to) personal information, including health and other sensitive information, about:

1. Pupils and parents and/or guardians (parents) before, during and after the course of a pupil's enrolment at the school
  - Name
  - Contact details (including next of kin)
  - Date of birth
  - Gender
  - Language background
  - Previous school
  - Religion
  - Parents' education, occupation and language background
  - Medical information (e.g. Details of disability and/or allergies, absence notes, medical reports and names of doctors)
  - Conduct and complaint records, or other behaviour notes, and school reports
  - Information about referrals to government welfare agencies
  - Counselling reports;
  - Health fund details and Medicare number
  - Any court orders
  - Volunteering information
  - And photos and videos at school events
  - Other related information.
2. Members
  - Name
  - Contact details (including next of kin)
  - Date of birth
  - Gender
  - Language background
  - Previous school
  - Religion
  - Church membership and status
  - Financial data (as related to FRSA membership status)
  - Conduct and complaint records, or other notes
  - Volunteering information
  - Other related information

3. Job applicants, staff members, volunteers and contractors, including:
  - Name
  - Contact details (including next of kin)
  - Date of birth
  - Religion
  - Information on job application
  - Professional development history
  - Salary and payment information
  - Including superannuation details
  - Medical information (e.g. Details of disability and/or allergies, and medical certificates)
  - Complaint records and investigation reports
  - Leave details
  - Photos and videos at school events
  - Workplace surveillance information
  - Work emails and private emails (when using work email address) and internet browsing history
  - Other related information.
4. Other people who come into contact with the school
  - Including name and contact details
  - Any other information necessary for the particular contact with the school.

#### **Personal Information provided by an individual:**

The FRSA and a school will generally collect personal information held about an individual by way of forms filled out by Members, Parents or pupils, face-to-face meetings and interviews, emails, and telephone calls. On occasions people other than Parents and pupils provide personal information.

#### **Personal Information provided by other people:**

In some circumstances a school may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

#### **Exception in relation to employee records:**

Under the Privacy Act the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the school's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the FRSA, school and employee.

The FRSA and schools handle staff health records in accordance with the Privacy Principles in the Health Records Act.

#### **How will the FRSA and schools use personal information?**

The FRSA and a school will use personal information it collects for the primary purpose of achieving the objects of the FRSA as set out in the Constitution (Section 1.3). Examples of such activities are outlined in the following section. Consistent with Australian Privacy Principle 6, the FRSA and a school may use personal information for a secondary use where an individual has consented to the disclosure or an individual would reasonably expect the information to be disclosed.

**Pupils, Parents and Members:**

In relation to personal information of Pupils, Parents and Members, the FRSA's and a school's primary purpose of collection is to enable the FRSA and schools to comply with the FRSA Constitution and provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the school.

This includes satisfying the needs of Members, Parents, the needs of the pupil and the needs of the FRSA and school throughout the whole period the pupil is enrolled at the school. The purposes for which FRSA and a school uses personal information of pupils and Parents and Members include:

- To keep parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines
- To keep members informed about matters relating to the operation of the FRSA and its schools through correspondence, newsletters and magazines
- Day-to-day administration
- Looking after pupils' educational, social, spiritual and medical wellbeing
- Managing membership, tuition and other related fees
- Seeking donations and marketing for the school
- To satisfy the FRSA's and the school's legal obligations
- Allow the school to discharge its duty of care.

In some cases where a school requests personal information about a pupil or Parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

**Job applicants and contractors:**

In relation to personal information of job applicants and contractors, the FRSA's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

The purposes for which a school uses personal information of job applicants and contractors include:

- Administering the individual's employment or contract, as the case may be
- For insurance purposes
- Satisfying the FRSA's and the school's legal obligations, for example, in relation to child protection legislation.

**Volunteers:**

A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, to enable the FRSA, school, and the volunteers to work together.

**Marketing and fundraising:**

The FRSA and Schools treat marketing and seeking donations for the future growth and development of the school as an important part of ensuring that the school continues to be a quality learning environment in which both pupils and staff thrive.

Parents, staff, contractors and other members of the wider school community may from time to time receive fundraising information.

School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

**Exception in relation to related schools:**

The Privacy Act allows each school, being legally related to each of the other schools conducted by the FRSA to share information with other schools conducted by the FRSA. Other FRSA schools may then only use this information for the purpose for which it was originally collected by the FRSA. This allows schools to transfer information between them, for example, when a pupil transfers from a FRSA school to another school conducted by the FRSA.

**Who might a school disclose personal information to and store information with?**

A school may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- Other schools and teachers at those schools
- The local Free Reformed Church
- Government departments (including for policy and funding purposes)
- People providing educational, support and health services to the school, including specialist visiting teachers, coaches, volunteers, and counsellors
- Providers of learning and assessment tools
- Assessment and educational authorities, including the Australian curriculum, assessment and reporting authority (Acara) and NAPALAN test administration authorities (who will disclose it to the entity that manages the online platform for NAPLAN)
- People providing administrative and financial services to the school
- Recipients of school publications, such as newsletters and magazines
- Pupils' parents or guardians
- Anyone an individual authorises the school to disclose information to
- Anyone to whom we are required or authorised to disclose the information by law, including child protection laws.

**Sending and storing information overseas:**

A school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, a school will not send personal information about an individual outside Australia without:

- Obtaining the consent of the individual (in some cases this consent will be implied)
- Otherwise complying with the Australian privacy principles or other applicable privacy legislation.

The school may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's server which may be situated outside Australia.

An example of such a cloud service provider is Office 365. Microsoft provides Office 365 and stores and processes limited personal information for this purpose. School personnel and the FRSA staff and their service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering Office 365 and ensuring its proper use.

**How does the FRSA and a school treat sensitive information?**

'Sensitive information' means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical



beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless the individual agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

### **Management and security of personal information**

The FRSA's and the schools' staff are required to respect the confidentiality of pupils', Parents' and Members' personal information and the privacy of individuals. The FRSA and each school has in place steps to protect the personal information the FRSA and each school holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

### **Access and correction of personal information**

Under the Commonwealth Privacy Act 1988 an individual has the right to seek and obtain access to any personal information which the FRSA or a school holds about them and to advise the FRSA or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act.

Pupils will generally be able to access and update their personal information through their Parents, but older pupils may seek access and correction themselves. There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or to update any personal information the FRSA or a school holds about individual or an individual's dependent child, please contact the school's Principal or FRSA Administration Manager by telephone or in writing.

The school may require an individual to verify their identity and specify what information is required. The school may charge a fee to cover the cost of verifying the application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the school will advise the likely cost in advance.

If the FRSA or school cannot provide an individual with access to that information, the FRSA or school will provide a written notice explaining the reasons for refusal.

### **Consent and rights of access to the personal information of pupils**

The FRSA respects every Parent's right to make decisions concerning their child's education. Generally, a school will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. A school will treat consent given by Parents as consent given on behalf of the pupil and notice to Parents will act as notice given to the pupil.

Parents may seek access to personal information held by a school or the FRSA about them or their child by contacting the school's Principal or FRSA Administration Manager by telephone or in writing. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the pupil.

A school may, at its discretion, on the request of a pupil grant that pupil access to information held by the school about them or allow a pupil to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances warrant it.

### **Enquiries and complaints**

If an individual would like further information about the way the FRSA or a school manages the personal information it holds or an individual wishes to complain that they believe that the FRSA or a school has breached the Australian Privacy Principles, please contact the school's Principal or the FRSA Administration Manager by writing or telephone. The FRSA or the school will investigate any complaint and will notify the individual of a decision in relation to their complaint as soon as is practicable after it has been made.

### **Supporting documentation**

The Privacy Compliance Manual (January 2018 – and updated from time to time) produced by the National Catholic Education Commission and Independent Schools Council of Australia provides a comprehensive overview of the Australian Privacy Principles and should be used in conjunction with this fact sheet and associated policy and procedure.

## Appendix 2

## Data Breach Response Plan

### Introduction

The template plan sets out the procedure to manage a School's or the FRSA's response to the actual or suspected unauthorised access to or disclosure or loss of personal information (**Data Breach**). The School and/or FRSA will need to adapt this template to their circumstances and may also wish to seek guidance from the Association of Independent Schools – Western Australia. Further guidance about responding to a Data Breach and an eligible data breach (**EDB**) under the notifiable data breaches scheme (**NDB Scheme**) is contained in Privacy Manual.

### Response plan

In the event of a Data Breach, School personnel must adhere to the four-phase process set out below (as described in the Office of the Australian Information Commissioner's (**OAIC**) *Notifiable Data Breaches scheme: Resources for agencies and organisations*.) It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought if necessary.

#### Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the Principal or Administration Manager. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. The school Principal or FRSA Administration Manager must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

#### Risk Level Description

Risk level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

4. Where a **High Risk** incident is identified, the school Principal or FRSA Administration Manager must consider if any of the affected individuals should be notified immediately where serious harm is likely.

5. The School Principal and/or Administration Manager must escalate **High Risk** and **Medium Risk** Data Breaches to the response team (whose details are set out at the end of this protocol).

6. If there could be media or stakeholder attention because of the Data Breach, it must be escalated to the response team.

**Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely**

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.

2. The response team is to work to evaluate the risks associated with the Data Breach, including by:

- a. Identifying the type of personal information involved in the Data Breach
- b. Identifying the date, time, duration, and location of the Data Breach
- c. Establishing who could have access to the personal information
- d. Establishing the number of individuals affected
- e. Establishing who the affected, or possibly affected, individuals are.

3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an EDB.

4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.

5. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

**Phase 3. Consider Data Breach notifications**

6. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.

7. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.

8. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.

9. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.

**Phase 4. Take action to prevent future Data Breaches**

10. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.

11. The Administration Manager must enter details of the Data Breach and response taken into a Data Breach log. The CEO in collaboration with the Administration Manager must, every year, review the Data Breach log to identify any reoccurring Data Breaches.

12. The FRSA CEO must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.

13. The FRSA CEO must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.

14. The school Principal and/or Administration Manger must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

### **Response Team**

The response team will include as a minimum the following members:

1. CEO of the FRSA
2. School Principal (if relevant) i.e. a School related breach
3. Administration Manager (if relevant) i.e. a FRSA related breach
4. A member of the IT staff.

The response team may appoint additional members as required.